

---

## **OLR Bill Analysis**

**sSB 159 (File 330, as amended by Senate "A")\***

### ***AN ACT CONCERNING EMPLOYEE PRIVACY.***

#### **SUMMARY:**

This bill prohibits an employer from requesting or requiring an employee or job applicant to provide the employer with his or her password or other access to a personal on-line account. It also bans an employer from (1) firing, disciplining, or otherwise penalizing an employee or applicant who refuses to provide this information and (2) firing or retaliating against an employee who files a complaint under the bill. It does not indicate where complaints will be filed or what body investigates them.

The bill provides exceptions for accounts and devices the employer provides and for certain types of investigations. It excludes from covered employers any state or local law enforcement agency conducting a preemployment personnel investigation or review.

\*Senate Amendment "A" eliminates the enforcement provision and (1) adds the ban on employers failing to hire a person solely for refusing to provide a password or other means of accessing a personal on-line account, (2) excludes state and local law enforcement from covered employers, (3) adds the exceptions to the ban, (4) exempts employers from any liability for failing to ask employees or applicants for access to personal on-line accounts, (5) adds a definition for "electronic communications device," and (6) adds other employer provisions.

EFFECTIVE DATE: October 1, 2013

#### **BAN ON REQUESTING PASSWORDS OR ACCOUNT ACCESS**

The bill, with certain exceptions described below, bans an employer

or prospective employer from requesting or requiring that an employee or applicant provide the employer or prospective employer with a user name, password, or any other authentication needed for accessing a personal on-line account. It defines “applicant” as anyone actively seeking employment from an employer, and “employer” means anyone engaged in business who has employees, including the state and any of its political subdivisions.

Under the bill, “personal on-line account” means an on-line account used by an employee or applicant exclusively for personal purposes and unrelated to any business purpose of the employer or prospective employer, including e-mail, social media, and retail-based Internet web sites. It does not include any account created, maintained, used, or accessed by an employee or applicant for business-related purposes or for a business purpose of the employer or prospective employer.

The bill bans employers from discharging, disciplining, discriminating against, retaliating against, or otherwise penalizing any employee or applicant who:

1. refuses or declines to provide the employer with a user name, password, or any other authentication for accessing his or her personal on-line account or
2. files any verbal or written complaint with a public or private body or court concerning the employer’s violation of the ban on asking for personal account access.

The bill also prohibits an employer from failing or refusing to hire any employee or applicant because he or she refused to provide a user name, password, or other means for accessing a personal on-line account.

The bill does not specify where complaints are filed or what body is responsible for investigating them.

#### **EXCEPTIONS TO THE BAN**

The bill provides a number of exceptions to the ban based on certain

circumstances. It permits an employer to request or require that an employee or applicant provide access to:

1. any account or service (a) provided by the employer or by virtue of the employee's work relationship with the employer or (b) that the employee uses for business purposes or
2. any electronic communications device the employer supplied or paid for, in whole or in part.

The bill defines "electronic communications device" as any electronic device capable of transmitting, accepting, or processing data, including a computer, computer network and computer system, as defined in state law, and a cellular or wireless telephone.

It also allows exceptions, with limitations, for investigations. It does not prevent an employer from conducting an investigation:

1. to ensure compliance with (a) applicable state or federal laws, (b) regulatory requirements, or (c) prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee or applicant's personal on-line account or
2. based on the receipt of specific information about an employee or applicant's unauthorized transfer of the employer's proprietary information, confidential information, or financial data to or from a personal on-line account operated by an employee, applicant, or other source.

While the bill requires the employee to provide access to the account for purposes of these investigations, it prohibits the employer from requiring the disclosure of the user name, password, or other means of accessing the personal on-line account.

The bill permits an employer to discharge, discipline, or otherwise penalize an employee or applicant who transferred, without the employer's permission, the employer's proprietary information, confidential information, or financial data to or from the employee or

applicant's personal on-line account.

***Monitoring and Blocking Data***

The bill allows an employer to monitor, review, access, or block electronic data stored on an electronic communications device paid for in whole or in part by the employer or traveling through or stored on an employer's network, in compliance with state and federal law.

***Self-Regulatory Organizations***

The bill specifies that it does not prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules for self-regulatory organizations.

**COMMITTEE ACTION**

Labor and Public Employees Committee

Joint Favorable

Yea 7      Nay 3      (03/19/2013)

Judiciary Committee

Joint Favorable

Yea 17      Nay 14      (05/01/2013)